

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-144756
 (43)Date of publication of application : 25.05.2001

(51)Int.CI. H04L 12/22
 H04L 9/32
 H04L 12/46
 H04L 12/28
 H04L 12/66
 H04L 12/56

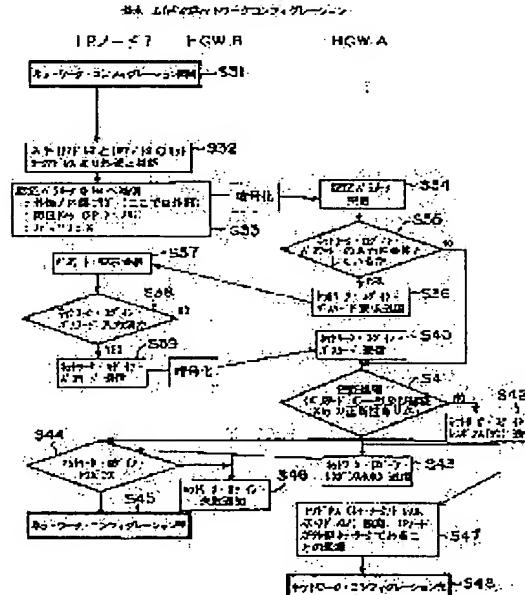
(21)Application number : 11-327247 (71)Applicant : SHARP CORP
 (22)Date of filing : 17.11.1999 (72)Inventor : KIMURA SHINYA
 KOBAYASHI YUTAKA

(54) NETWORK CONFIGURATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To network-configure an optional IP node connected onto an IP network as a desired IP node.

SOLUTION: In this network configuration system of the IP node connected to a network through a public Internet and a gateway GW, the IP node 7 has a means reading authentication information when a card-shaped recording medium on which the authentication information and the address of a home gateway are recorded is inserted, a means (S33) enciphering the read authentication information and transmitting the authentication information to the GW, and means (S44 and S45) network-configuring the IP node when the authentication information transmitted from the GW is decided as proper, and the GW has a means (S41) which collates the transmitted authentication information with information for authentication stored in the GW and decides the identify of the authentication information and means (S42 and S43) transmitting the decision result of the identify of the authentication information to the IP node.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

BEST AVAILABLE COPY

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-144756

(P2001-144756A)

(43) 公開日 平成13年5月25日 (2001.5.25)

(51) Int.Cl.⁷
H 04 L 12/22
9/32
12/46
12/28
12/66

識別記号

F I
H 04 L 11/26
9/00
11/00
11/20

テマコード*(参考)
5 J 10 4
6 7 3 A 5 K 0 3 0
3 1 0 C 5 K 0 3 3
B
1 0 2 A

審査請求 未請求 請求項の数 4 OL (全 15 頁) 最終頁に続く

(21) 出願番号 特願平11-327247

(22) 出願日 平成11年11月17日 (1999.11.17)

(71) 出願人 000003049

シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 木村 真也

大阪府大阪市阿倍野区長池町22番22号 シ
ヤープ株式会社内

(73) 発明者 小林 裕

大阪府大阪市阿倍野区長池町22番22号 シ
ヤープ株式会社内

(74) 代理人 100108338

弁理士 七條 耕司 (外1名)

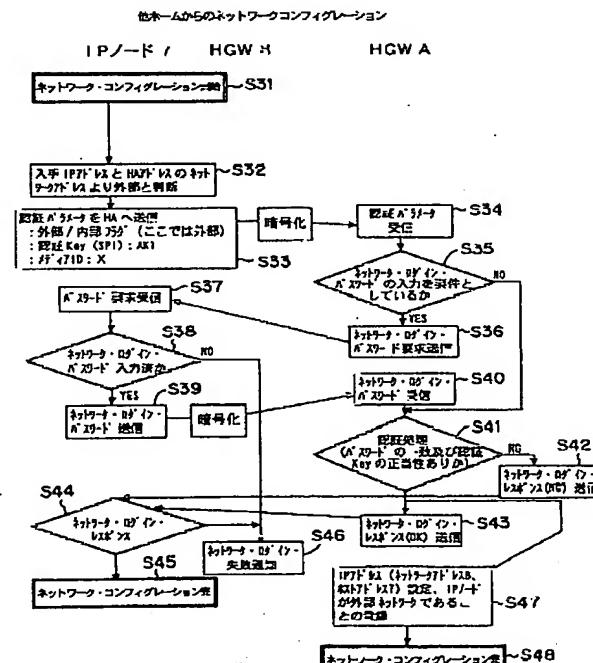
最終頁に続く

(54) 【発明の名称】 ネットワーク・コンフィギュレーション方式

(57) 【要約】

【課題】 IPネットワーク上に接続される任意のIPノードを、所望のIPノードとしてネットワーク・コンフィギュレーションする。

【解決手段】 公衆インターネットとゲートウェイGWを介しネットワークに接続されるIPノードのネットワーク・コンフィギュレーション方式において、前記IPノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着時、前記認証情報を読み取る手段と、読み取った認証情報を暗号化して前記GWに送信する手段(S33)と、前記GWから送信された前記認証情報が正当であると判断された時はIPノードをネットワーク・コンフィギュレーションする手段(S44, S45)とを有し、前記GWは、送信された認証情報をGWが記憶している認証用情報と照合して認証情報の正当性を判断する手段(S41)と、前記IPノードに前記認証情報の正当性の判断結果を送信する手段(S42, S43)とを有することを特徴とする。



【特許請求の範囲】

【請求項1】 公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークに接続されるIPノードのネットワーク・コンフィギュレーション方式において、

前記IPノードは、認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断されたときは当該IPノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報を照合して認証情報の正当性を判断する手段と、前記IPノードに前記認証情報の正当性の判断結果を送信する手段とを有することを特徴とするネットワーク・コンフィギュレーション方式。

【請求項2】 公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークに接続されるIPノードのネットワーク・コンフィギュレーション方式において、

前記IPノードは、認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、当該IPノードから入力されたパスワードを前記ホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断され、かつ前記ホームゲートウェイから送信された前記パスワードの一貫性の判断結果について一致していると判断されたときは当該IPノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報を照合して認証情報の正当性を判断すると共に、前記送信されたパスワードを当該ホームゲートウェイが記憶している記憶パスワードと対比してパスワードの一貫性を判断する手段と、前記IPノードに前記認証情報の正当性の判断結果および前記パスワードの一貫性の判断結果を送信する手段とを有することを特徴とするネットワーク・コンフィギュレーション方式。

【請求項3】 公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークと、前記公衆インターネットとゲートウェイを介して相互接続されるネットワークに接続されるIPノードのネットワーク・コンフィギュレーション方式において、
前記IPノードは、認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記ゲートウェイに送信する手段と、前記ゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ゲートウェイが記憶している認証用情報を照合して認証情報の正当性を判断すると共に、前記送信されたパスワードを当該ゲートウェイが記憶している記憶パスワードと対比してパスワードの一貫性を判断する手段と、前記IPノードに前記認証情報の正当性の判断結果および前記パスワードの一貫性の判断結果を送信する手段とを有することを特徴とするネットワーク・コンフィギュレーション方式。

ドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断されたときは当該IPノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報を照合して認証情報の正当性を判断する手段と、前記IPノードに前記認証情報の正当性の判断結果を送信する手段とを有することを特徴とするネットワーク・コンフィギュレーション方式。

【請求項4】 公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークと、前記公衆インターネットとゲートウェイを介して相互接続されるネットワークに接続されるIPノードのネットワーク・コンフィギュレーション方式において、

前記IPノードは、認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、当該IPノードから入力されたパスワードを前記ホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断され、かつ前記ホームゲートウェイから送信された前記パスワードの一貫性の判断結果について一致していると判断されたときは当該IPノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報を照合して認証情報の正当性を判断すると共に、前記送信されたパスワードを当該ホームゲートウェイが記憶している記憶パスワードと対比してパスワードの一貫性を判断する手段と、前記IPノードに前記認証情報の正当性の判断結果および前記パスワードの一貫性の判断結果を送信する手段とを有することを特徴とするネットワーク・コンフィギュレーション方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、IPネットワーク上に接続される任意のIPノードを、所望のIPノードとして容易にコンフィギュレーションすることを可能にしたネットワーク・コンフィギュレーション方式に関する。

【0002】

【従来の技術】 従来、LAN等のセキュリティが必要なネットワークに対して、パーソナルコンピュータ（以下、PCという）等をIPノードとしてLAN上にコン

フィギュレーションするためには、PC毎に何らかのマニュアルによりセットアップ作業が必要であり、また、IPネットワーク上の外部のネットワークに接続したPCから前記LANにログインする場合には、PCに前記LAN上のリモートアクセスサーバと認証手続きをするためのパスワード設定やソフトウェアを実装するとともに、マニュアルによりログインするための入力作業を必要とする。また、モバイルIP(Mobile IP)のプロトコルで前記LANに接続する場合は、モバイルIPが前記プロトコルを実装しているとともに、前記LAN上のホームエージェント(Home Agent)等の情報が設定されている必要がある。

【0003】特開平11-252068号公報には、他の通信装置上に自己のデータ通信環境を設定し、遠隔地からでも特定の相手側通信装置に安全かつ最適にアクセスするために、自己のデータ通信を構築するための情報と認証用の情報を記録したICカードを通信装置にセットして本人証とカード認証を行い、通信中継装置において通信装置から取得した情報から相手側通信装置を特定し、その相手側通信装置の公開鍵を用いて電子署名を復号化し、通信装置の通信中継装置に対する正当性を認証し、通信装置、通信中継装置、相手側通信装置間で通信可能とする技術が開示されている。

【0004】

【発明が解決しようとする課題】しかし、上記のLAN等のセキュリティにより保護されているネットワークに外部ネットワークからログインするためには、認証を含んだリモートアクセスのためのソフトウェアとログインのためのパスワードやIDを設定してあるPC自体を持ち歩くか、また、モバイルIPの場合も、モバイルIPのプロトコルを有するソフトウェアとホームエージェントへの登録のためのアドレスが設定されているモバイルIPを持ち歩かなければならず、その度に、ソフトウェアの設定をする必要があり面倒であった。

【0005】また、上記公報の技術は、データ通信を構築するための情報と認証用の情報を記録したICカードを通信装置に装着して、通信装置側でデータ通信環境の構築と認証を行うようにして、データ通信のためのユーザの利便性を高めようとするものであるが、ICカード内に認証に係わる情報が多く、また認証処理のために通信装置、通信中継装置、相手側通信装置間での処理を必要としシステムが複雑化する問題がある。

【0006】本発明の目的は、上記の種々の問題点に鑑みて、カード等の記憶メディアにログインしたいネットワークへのログイン情報を記憶することにより、前記ネットワークまたはIPネットワーク上の他のネットワークの任意のIPノードに前記記憶メディアを装着することにより、装着されたIPノードを自らのネットワーク上のIPノードとして利用できるように自動的にコンフィギュレーションすることを可能にしたネットワーク・

コンフィギュレーション方式を提供することにある。

【0007】

【課題を解決するための手段】本発明は、上記の課題を解決するために、次のような手段を採用した。

【0008】第1の手段は、公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークに接続されるIPノードのネットワーク・コンフィギュレーション方式において、前記IPノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断されたときは当該IPノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断する手段と、前記IPノードに前記認証情報の正当性の判断結果を送信する手段とを有することを特徴とする。

【0009】第2の手段は、公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークに接続されるIPノードのネットワーク・コンフィギュレーション方式において、前記IPノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、当該IPノードから入力されたパスワードを前記ホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断され、かつ前記ホームゲートウェイから送信された前記パスワードの一一致の判断結果について一致していると判断されたときは当該IPノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断すると共に、前記送信されたパスワードを当該ホームゲートウェイが記憶している記憶パスワードと対比してパスワードの一一致の判断する手段と、前記IPノードに前記認証情報の正当性の判断結果および前記パスワードの一一致の判断結果を送信する手段とを有することを特徴とする。

【0010】第3の手段は、公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークと、前記公衆インターネットとゲートウェイを介して相互接続されるネットワークに接続されるIPノードのネットワーク・コンフィギュレーション方式において

て、前記IPノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断されたときは当該IPノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断する手段と、前記IPノードに前記認証情報の正当性の判断結果を送信する手段とを有することを特徴とする。

【0011】第4の手段は、公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークと、前記公衆インターネットとゲートウェイを介して相互接続されるネットワークに接続されるIPノードのネットワーク・コンフィギュレーション方式において、前記IPノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、当該IPノードから入力されたパスワードを前記ホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断され、かつ前記ホームゲートウェイから送信された前記パスワードの一一致性の判断結果について一致していると判断されたときは当該IPノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断すると共に、前記送信されたパスワードを当該ホームゲートウェイが記憶している記憶パスワードと対比してパスワードの一一致性を判断する手段と、前記IPノードに前記認証情報の正当性の判断結果および前記パスワードの一一致性の判断結果を送信する手段とを有することを特徴とする。

【0012】

【発明の実施の形態】本発明の第1の実施形態を図1乃至図5を用いて説明する。

【0013】はじめに、本実施形態に係るネットワーク・コンフィギュレーションに先だって、記憶メディアへのログイン情報の入力処理について図1および図2を用いて説明する。

【0014】図1は、カード状記憶媒体として、購入されて未だログイン情報が書き込まれていない空白状態にあるネットワーク・コンフィギュレーション・メディア

を示す図であり、図2は、任意のネットワークに設けられるホームゲートウェイHGW(Home Gateway)によって、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディアを示す図である。

【0015】これらの図において、ホームゲートウェイHGWは、インターネット等の公衆インターネットとLAN等で構築されたホームネットワーク間のデータの受け渡し機能を有し、ここでは、ルータ(Router A)と、状況に応じて意図を理解して自立的な判断に基づいて各種の処理を行い、ホームネットワークAでモバイルIP通信をサポートするホームエージェント(Home Agent)と共に、ネットワーク・コンフィギュレーション・メディア0～3にログイン情報を書き込む装置と書き込むためのネットワーク管理テーブルを備えている。ネットワーク・コンフィギュレーション・メディア0～3は、購入時は、それぞれメディアID X～ID Wを有しているが、ホームエージェントHAのホームアドレスおよび認証キー(SPI:Security parameter Index)は空白の状態にある。

【0016】ネットワーク・コンフィギュレーション・メディア0～3への、ログイン情報の書き込みは、図2に示すように、ネットワーク管理テーブルを有するホームゲートウェイHGW Aに各ネットワーク・コンフィギュレーション・メディア0～3を装着することにより自動的に行われる。先ず、ホームゲートウェイHGW Aに各ネットワーク・コンフィギュレーション・メディア0～3からメディアID X～ID Wが入力され、それに応じて、各ネットワーク・コンフィギュレーション・メディア0～3に、それぞれホームエージェントHAのホームアドレスA、認証キー(SPI)AK1～AK4が付与される。さらに、必要に応じて、ネットワーク・ログイン・パスワードXX～ZZを付与するようにしてもよい。ネットワーク・ログイン・パスワードが付与されている場合は、ネットワーク・コンフィギュレーション・メディアの紛失時等において他人の不正使用を防止することができる。

【0017】次に、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディアを用いて、本実施形態に係るホームネットワークにおけるIPノードのネットワーク・コンフィギュレーションについて図3乃至図5を用いて説明する。

【0018】図3は、IPノード0にネットワーク・コンフィギュレーション・メディア0を装着してIPノード0をネットワーク・コンフィギュレーションしようとしている状態を示す図であり、図4は、IPノード0のネットワーク・コンフィギュレーションが終了した状態を示す図である。

【0019】これらの図において、ネットワークAは、

ルータAおよびホームアドレスAを有するホームエージェントHAからなるホームゲートウェイHWGを介してインターネット網に接続されている。IPノード1～3は、既にホームネットワークAに接続され、ホームゲートウェイHWGのルータAのDHCPサーバからIPアドレスであるA1～A3（ネットワークアドレスA・ホストアドレス0～3）を付与されたノードであり、IPノード0は、例えば、新規に購入される等して、ネットワークAに接続され、IPアドレスの割り当ておよびネットワーク・コンフィギュレーションを行うノードである。ネットワーク・コンフィギュレーション・メディア0は、メディアID Xを有し、既にホームアドレスA、および認証キー（SPI）AK1のログイン情報が入力されたものである。

【0020】図5は、ホームネットワークAにおいて、ネットワーク・コンフィギュレーション・メディア0を用いてIPノード0をネットワーク・コンフィギュレーションするための処理手順を示すフローチャートである。

【0021】ステップ1において、ホームネットワークAにIPノード0を接続し、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディア0をIPノード0に装着することによりネットワーク・コンフィギュレーションが開始される。ステップ2では、ホームエージェントHA AとIPノード0間でデータリンクレベルでの接続処理が行われ、データリンクが確立する。ステップ3では、ホームゲートウェイHWGAのルータAのDHCPサーバにより、IPノード0に対してIPアドレス（ネットワークアドレスA、ホストアドレス0）を割り当てる。ステップ4では、IPノード0は、入手したIPアドレス（ネットワークアドレスA、ホストアドレス0）とホームエージェントHA AのネットワークアドレスAとを対比して、IPノード0がホームネットワークA内部にあることを判断する。ステップ5では、IPノード0は認証パラメータをホームゲートウェイHWGのホームエージェントHA Aにデータを暗号化して送信する。送信内容は、IPノード0がホームネットワークA内部であることを示すフラグと、ネットワーク・コンフィギュレーション・メディア0から入手した認証キー（SPI）AK1、メディアID Xである。ステップ6でホームエージェントHA Aは認証パラメータを受信して、ステップ7で、ネットワーク・ログイン・パスワードが設定されている場合にネットワーク・ログイン・パスワードを必要とするか否かを判断する。ここで、ネットワーク・ログイン・パスワードは、外部フラグが立っているときのみ必要とするようにしてもよいし、また、内部／外部フラグに係わらず必要とするようにしてもよい。ステップ7においてネットワーク・ログイン・パスワードが必要と判断された場合は、ステップ8において、IPノード0に対して、ネッ

トワーク・ログイン・パスワードの送信を要求する。ステップ9でIPノード0がパスワード要求を受信すると、ステップ10で、ネットワーク・ログイン・パスワードの入力を確認し、ネットワーク・ログイン・パスワードが入力されている場合は、ステップ11でホームエージェントHA Aにネットワーク・ログイン・パスワードXXを暗号化して送信する。ネットワーク・ログイン・パスワードが入力されていない場合はステップ18においてネットワーク・ログインが失敗であることを知らせる。ステップ12でホームエージェントHA Aはネットワーク・ログイン・パスワードXXを受信し、ステップ13において、送信されたネットワーク・ログイン・パスワードXXおよび認証キー（SPI）AK1を、図2に示したネットワーク管理テーブルに記憶されているデータと対比して、パスワードの一致性および認証キーの正当性を判断する。一致性および正当性が認められない場合は、ネットワーク・ログイン・レスポンス（NG）をIPノード0に送信し、一致性および正当性が認められた場合は、ネットワーク・ログイン・レスポンス（OK）をIPノード0に送信する。ステップ16において、IPノード0はネットワーク・ログイン・レスポンスを受信し、それがネットワーク・ログイン・レスポンス（OK）の場合は、ステップ17においてIPノード0におけるネットワーク・コンフィギュレーションを完了し、ネットワーク・ログイン・レスポンス（NG）の場合は、ステップ18においてネットワーク・ログインが失敗であることを知らせる。また、ステップ13において、一致性および正当性が認められた場合は、さらにステップ19において、ホームネットワークA上のIPノード0のIPアドレス（ネットワークアドレスA、ホストアドレス0）を登録すると同時に、ネットワーク・コンフィギュレーション・メディア0が内部ネットワークにあることを登録し、ステップ20でネットワーク・コンフィギュレーションを完了する。

【0022】本実施形態によれば、上記のネットワーク・コンフィギュレーション・メディア0をIPノード0に装着しておくことにより、ネットワーク・コンフィギュレーションされた状態が保持される。ここでネットワーク・コンフィギュレーション・メディア0をIPノード0から外すと、ネットワーク・コンフィギュレーションは解除される。

【0023】なお、本実施形態では、新規に購入しIPノード0をホームネットワークAに接続する場合のコンフィギュレーションについて説明したが、既にネットワーク・コンフィギュレーションされているIPノード0に対して、ネットワーク・コンフィギュレーション・メディア0を装着してネットワーク・コンフィギュレーションしてもよく、その場合はネットワーク・コンフィギュレーション・メディア0に従って、ネットワーク・コンフィギュレーションされ、ネットワーク・コンフィギ

ュレーション・メディア0を外すと元のコンフィギュレーション状態に戻すことができる。

【0024】このように、本実施形態によれば、ホームネットワークAにおいて、新規のまたは任意のIPノードに対してネットワーク・コンフィギュレーション・メディアを装着することにより、自動的にIPノードをネットワーク・コンフィギュレーションすることができる。

【0025】次に、本発明の第2の実施形態を図6乃至図8を用いて説明する。

【0026】なお、ネットワーク・コンフィギュレーションに先立つネットワーク・コンフィギュレーション・メディアへのログイン情報の入力処理は第1の実施形態の場合と同じである。

【0027】図6は、IPノード7にネットワーク・コンフィギュレーション・メディア0を装着してネットワーク・コンフィギュレーションしようとしている状態を示す図であり、図7は、IPノード7に、ネットワーク・コンフィギュレーション・メディア0を装着してネットワーク・コンフィギュレーションが終了した状態を示す図である。

【0028】次に、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディア0を用いて、ホームネットワークA外の公衆インターネットに接続された他のネットワークBに接続されたIPノードにおけるネットワーク・コンフィギュレーションについて説明する。

【0029】図6および図7において、ホームネットワークAは、図3に示すものと比べてIPノード0が接続されていない以外は同じ構成であるので説明を省略する。ネットワークBは、ルータBおよびホームアドレスBを有するホームエージェントHAからなるホームゲートウェイHGW_Bを介してインターネット網に接続されている。ここで、IPノード7を含めIPノード4～7は、既にネットワークBに接続され、ホームゲートウェイHGW_BのルータBのDHCPサーバによりIPアドレス（ネットワークアドレスB、ホストアドレス4～ネットワークアドレスB、ホストアドレス7）を付与されたノードである。IPノード7は、これに操作者が携帯するネットワーク・コンフィギュレーション・メディア0を装着して、ネットワーク・コンフィギュレーションを行おうとするものであり、ネットワーク・コンフィギュレーション・メディア0には、第1の実施形態と同様に、メディアID_Xを有し、既にホームアドレスA、および認証キー（SPI）AK1のログイン情報が書き込まれたものである。

【0030】図8は、ネットワーク・コンフィギュレーション・メディア0を用いて、公衆ネットに接続されるホームネットワークA以外の他のネットワークBに接続されるIPノード7をネットワーク・コンフィギュレー

ションするための処理手順を示すフローチャートである。

【0031】本実施形態では、IPノード7は、既にネットワークBに接続されているので、ネットワークBのホームエージェントHA_BからIPアドレス（ネットワークアドレスB、ホストアドレス7）を付与されている。

【0032】ステップ31において、ネットワークBのIPノード7に、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディア0を装着することによりネットワーク・コンフィギュレーションが開始される。ステップ32では、IPノード7は、付与されているIPアドレス（ネットワークアドレスB、ホストアドレス7）とネットワーク・コンフィギュレーション・メディア0のホームエージェントHA_AのネットワークアドレスAとを対比して、IPノード7がホームネットワークAの外部にあることを判断する。ステップ33では、IPノード7は認証パラメータをホームエージェントHA_Aにデータを暗号化して送信する。送信内容は、IPノード7がネットワークA外部であることを示すフラグと、ネットワーク・コンフィギュレーション・メディア0から入手した認証キー（SPI）AK1、メディアID_Xである。ステップ34でホームエージェントHA_Aは認証パラメータを受信して、ステップ35で、ネットワーク・ログイン・パスワードが設定されている場合に入力することが要件になっているか否かを判断する。ここで、ネットワーク・ログイン・パスワードは、外部フラグが立っているときのみパスワードを必要とするようにしてもよいし、また、内部/外部フラグに係わらずパスワードを必要とするようにしてもよいし、また全く不要としてもよい。ネットワーク・ログイン・パスワードの入力を要件としている場合は、ステップ36において、IPノード7に対して、ネットワーク・ログイン・パスワードの送信を要求する。ステップ37でIPノード7がパスワード要求を受信すると、ステップ38で、ネットワーク・ログイン・パスワードの入力を確認し、ネットワーク・ログイン・パスワードが入力されている場合は、ステップ39でホームエージェントHA_Aにネットワーク・ログイン・パスワードXXを暗号化して送信する。ネットワーク・ログイン・パスワードを入力されていない場合は、ステップ46においてネットワーク・ログインが失敗であることを知らせる。ステップ40でホームエージェントHA_Aはネットワーク・ログイン・パスワードXXを受信し、ステップ41において、送信されたネットワーク・ログイン・パスワードXXおよび認証キー（SPI）AK1を、図2に示したネットワーク管理テーブルに記憶されているデータと対比して、パスワードの一致性および認証キーの正当性を判断する。一致性および正当性が認められない場合は、ネットワーク・ログイン・レスポンス（N

G) をIPノード7に送信し、一致性および正当性が認められた場合は、ネットワーク・ログイン・レスポンス(OK)をIPノード7に送信する。IPノード7はネットワーク・ログイン・レスポンスを受信した結果、ステップ44において、ネットワーク・ログイン・レスポンス(OK)を受信した場合は、ステップ45においてIPノード7におけるネットワーク・コンフィギュレーションを完了し、ネットワーク・ログイン・レスポンス(NG)の場合は、ステップ46においてネットワーク・ログインが失敗であることを知らせる。また、ステップ41において、一致性および正当性が認められた場合は、さらにステップ47において、外部ネットワークB上のIPノード7のIPアドレス(ネットワークアドレスB、ホストアドレス7)をトネリング先として登録し、同時にネットワーク・コンフィギュレーション・メディア0が外部ネットワークであることを登録し、ステップ48でネットワーク・コンフィギュレーションを完了する。なお、ここで、IPアドレス(ネットワークアドレスB、ホストアドレス7)は、ステップ33のIPアドレス7のホームエージェントHAへの認証パラメータの送信時に送信側IPアドレスとして入手することができる。これによって、公衆インターネット上の通信相手からIPノード7宛のデータは、ホームエージェントHAを経由してトネリングされてネットワークB上のIPノード7に転送される。

【0033】上記のごとく、本実施形態によれば、ホームネットワークA以外の他のネットワークBのIPノード7にネットワーク・コンフィギュレーション・メディア0を装着することにより、IPノード7をホームネットワークA上のIPノードと同様に利用できるように自動的にコンフィギュレーションすることができる。また、ネットワーク・コンフィギュレーション・メディア0をIPノード7に装着しておくことにより、ネットワーク・コンフィギュレーション状態が確保される。このように、ネットワークBに接続されているIPノード7はあたかもネットワークAに接続されているかのごとく使用することができ、ホームネットワークAに自由にアクセスすることができる。ここでネットワーク・コンフィギュレーション・メディア0をIPノード7から外すと、先のネットワーク・コンフィギュレーションは解除される。

【0034】

【発明の効果】本願第1の発明乃至第4の発明によれば、カード状記憶媒体は小型軽量に構成できるので、ユーザはこのカード状記憶媒体を持ち歩くことが可能となり、ユーザは、IPネットワーク上の任意のIPノードにこのカード状記憶媒体を装着することにより、ホーム

ネットワークまたはホームネットワーク以外のネットワークに接続されているIPノードを自動的にネットワーク・コンフィギュレーションすることができる。

【0035】また、少なくとも認証情報を記憶した記憶媒体を携帯するだけでよいので、従来技術のように、認証を含んだリモートアクセスのためのソフトウェアやとログインのためのパスワードやIDを設定してあるPC自体を持ち歩く必要がなくなる。

【0036】また、本願第2の発明および第4の発明によれば、ネットワーク・コンフィギュレーションの要件としてパスワードも付加することにより、カード状記憶媒体の紛失時等の不正使用を防止することができる。

【図面の簡単な説明】

【図1】購入されて未だログイン情報が書き込まれていない空白状態にあるネットワーク・コンフィギュレーション・メディアを示す図であり、

【図2】ホームゲートウェイHGW-Aによって、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディアを示す図である。

【図3】第1の実施形態に係るIPノード0にネットワーク・コンフィギュレーション・メディア0を装着してネットワーク・コンフィギュレーションしようとしている状態を示す図である。

【図4】第1の実施形態に係るIPノード0におけるネットワーク・コンフィギュレーションが終了した状態を示す図である。

【図5】第1の実施形態に係るホームネットワークAにおいて、ネットワーク・コンフィギュレーション・メディア0を用いてIPノード0をネットワーク・コンフィギュレーションするための処理手順を示すフローチャートである。

【図6】第2の実施形態に係るIPノード7にネットワーク・コンフィギュレーション・メディア0を装着してネットワーク・コンフィギュレーションしようとしている状態を示す図である。

【図7】第2の実施形態に係るIPノード7におけるネットワーク・コンフィギュレーションが終了した状態を示す図である。

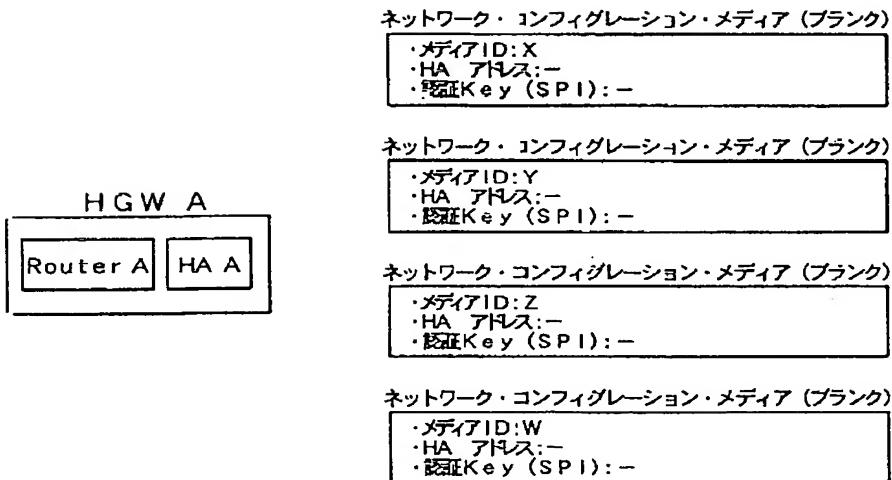
【図8】第2の実施形態に係るネットワーク・コンフィギュレーション・メディア0を用いてホームネットワーク以外の他のネットワークのIPノード7をネットワーク・コンフィギュレーションするための処理手順を示すフローチャートである。

【符号の説明】

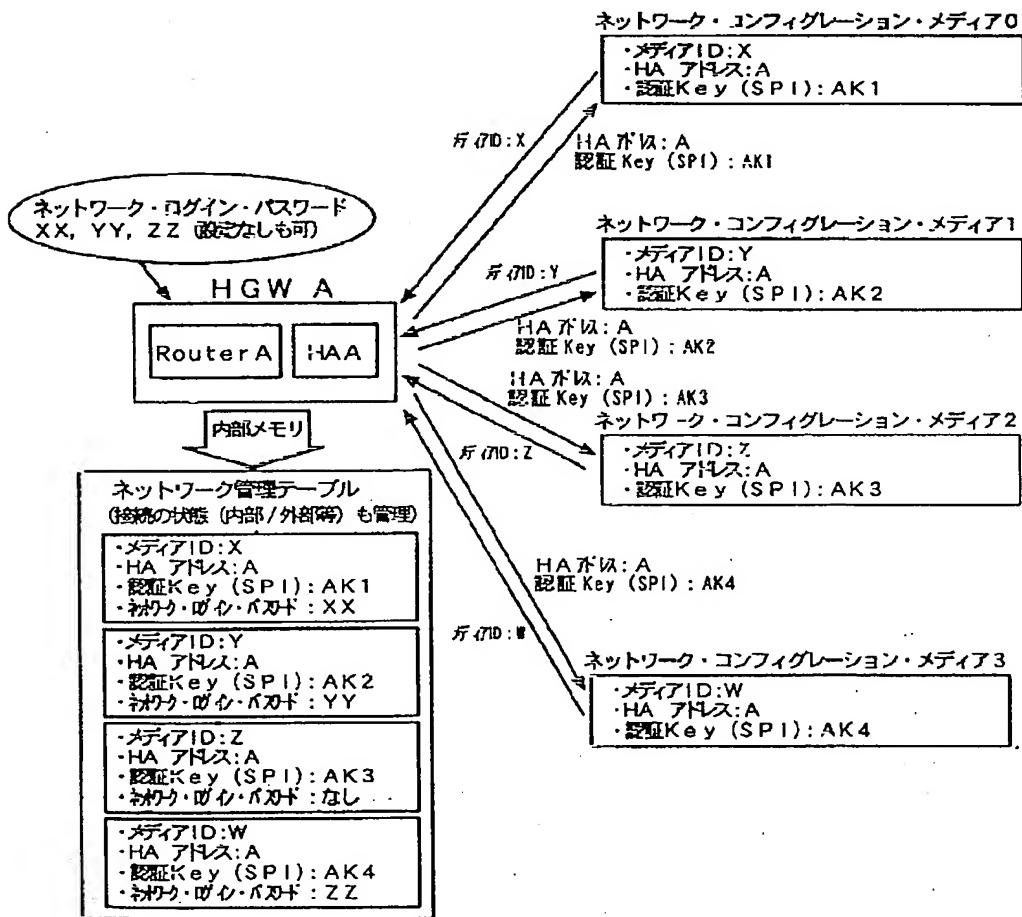
HGW ホームゲートウェイ

HA ホームエージェント

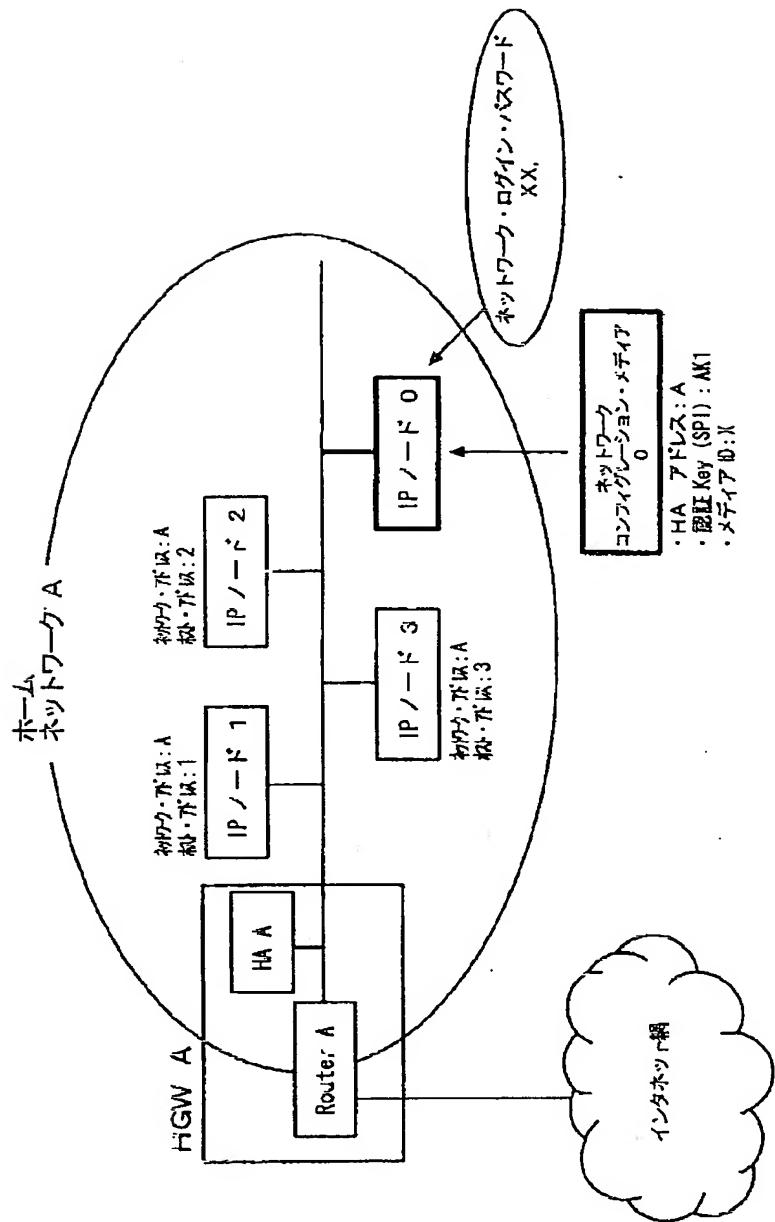
【図1】



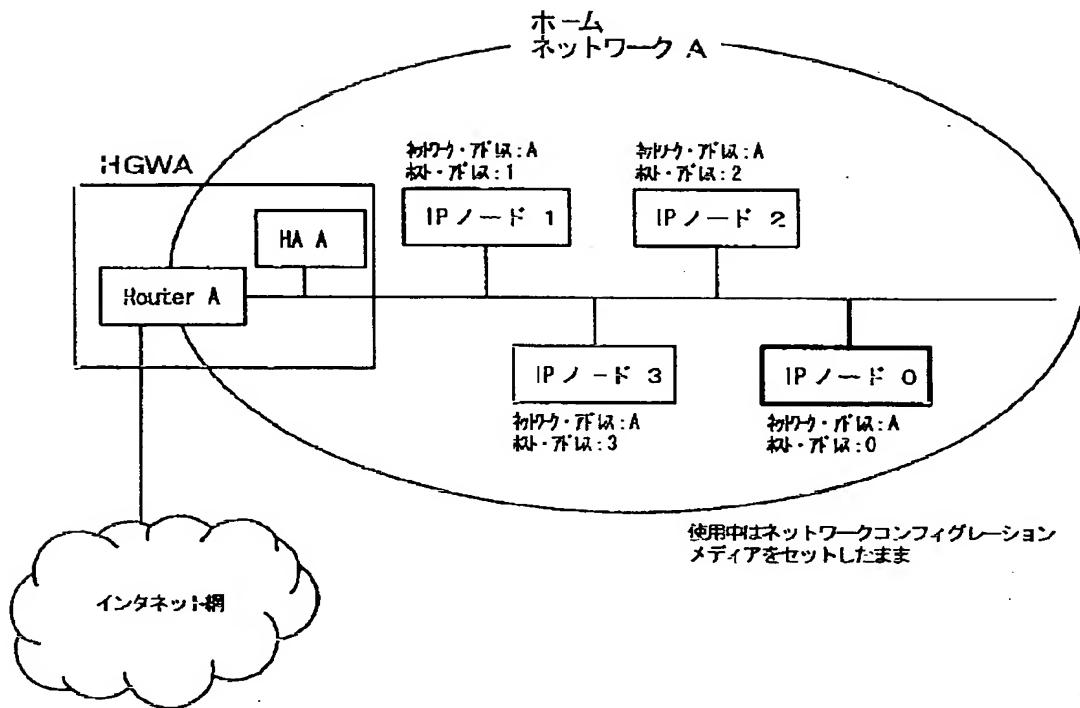
【図2】



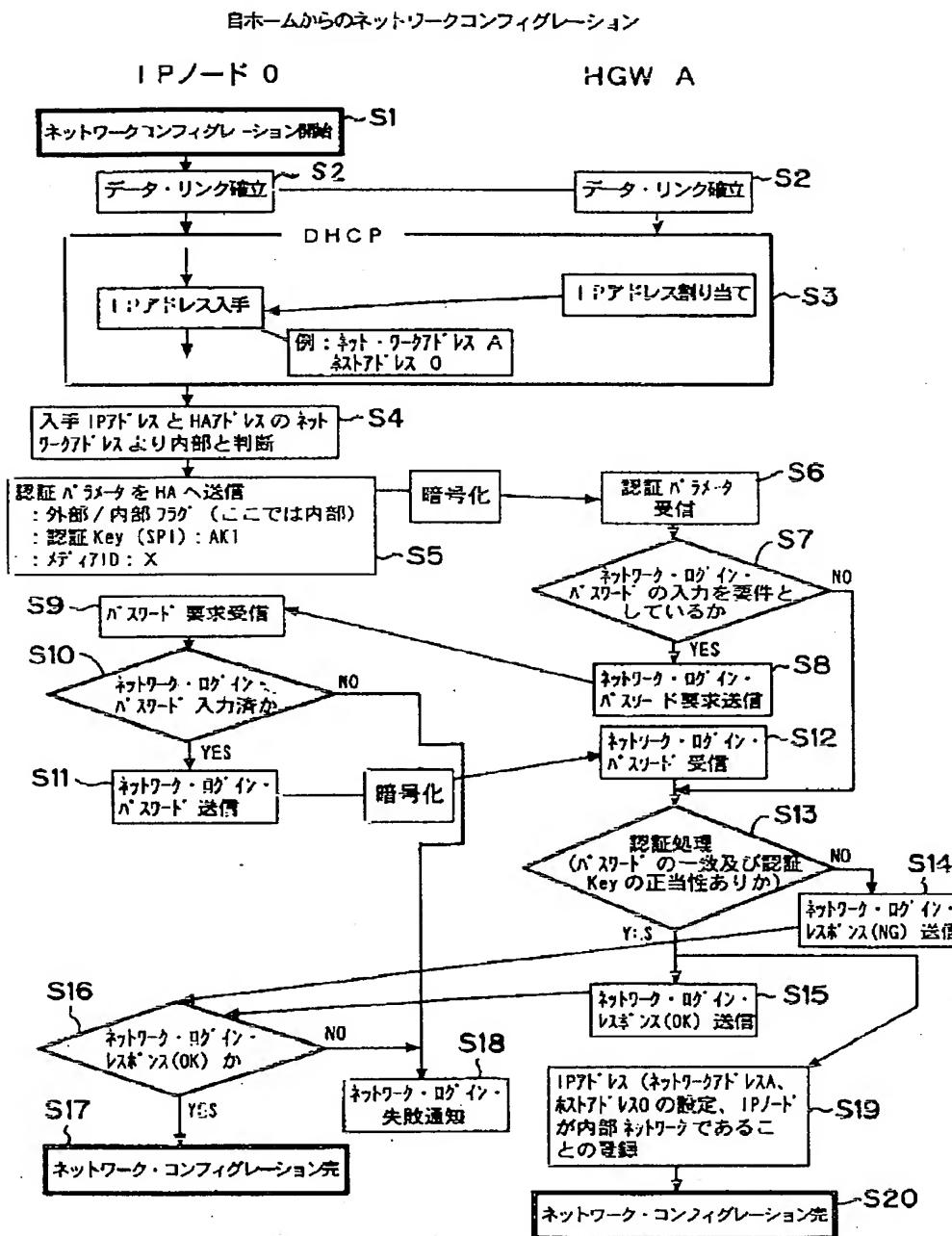
【図3】



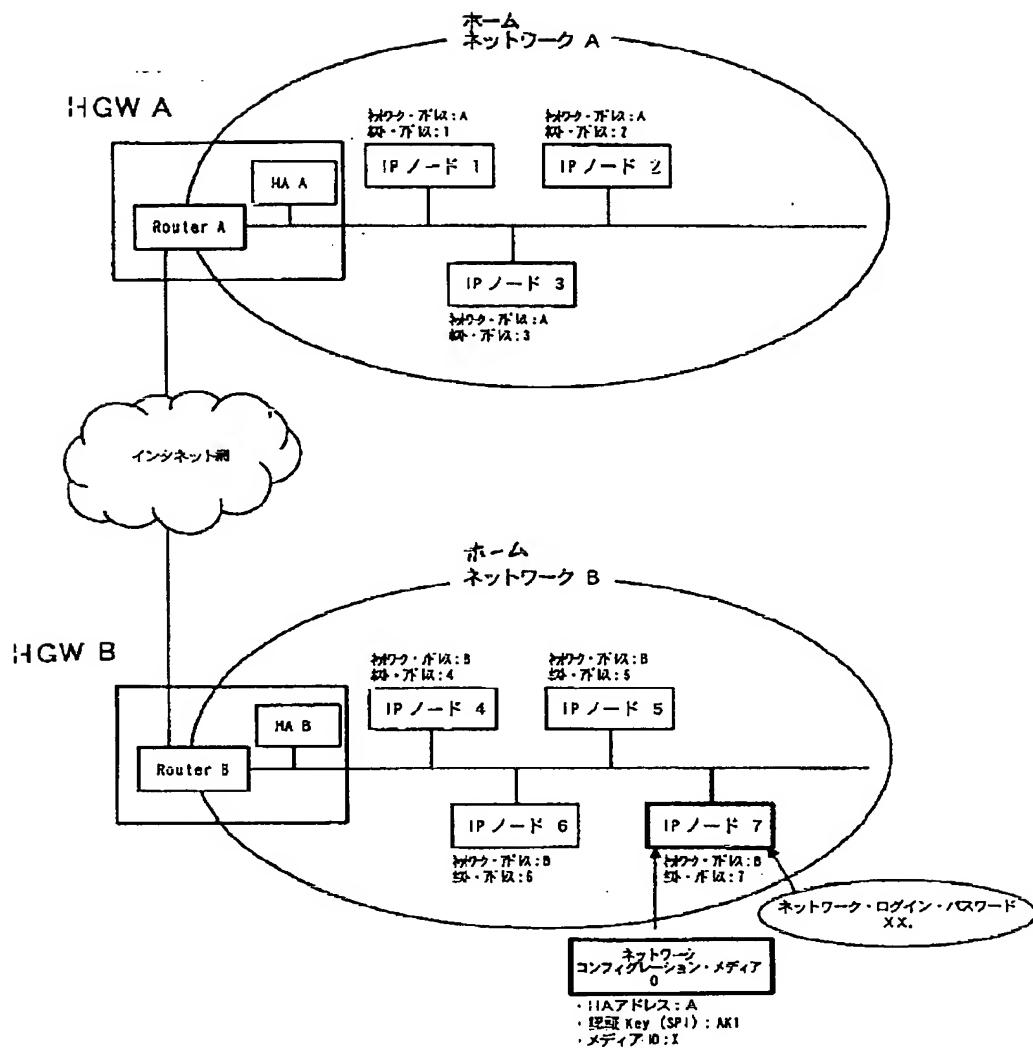
【図4】



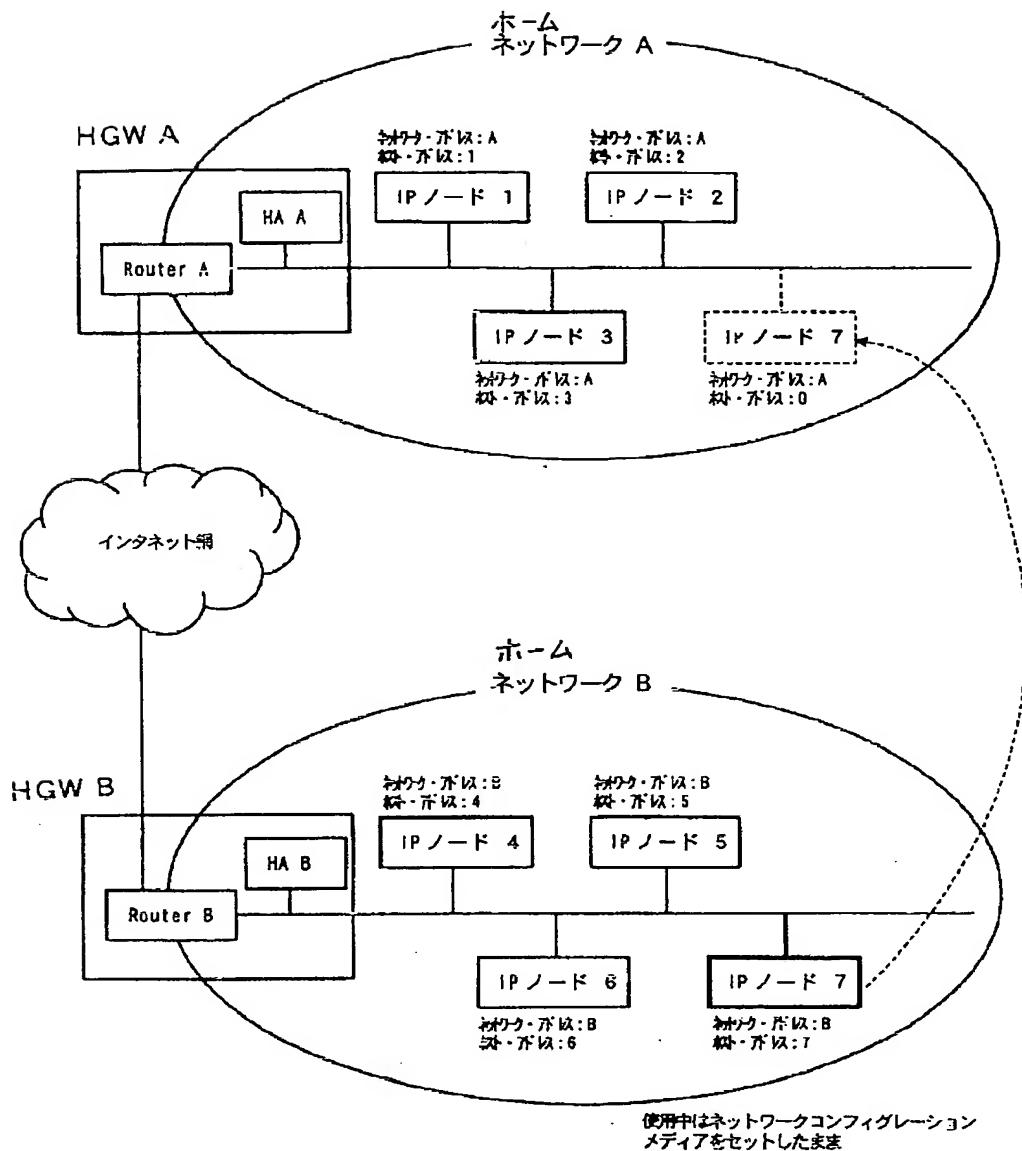
【図5】



【図6】

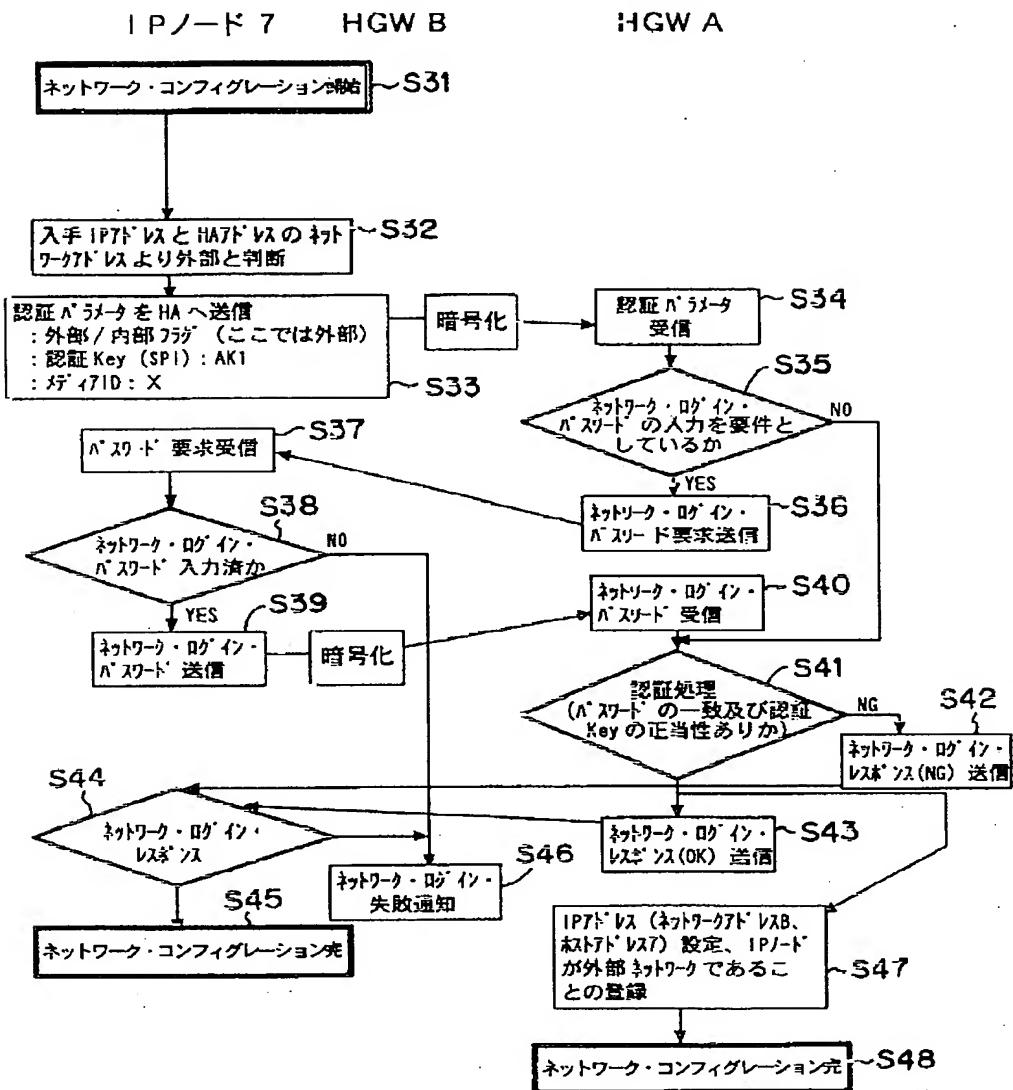


【図7】



【図8】

他ホームからのネットワークコンフィグレーション



フロントページの続き

(15) 01-144756 (P2001-144756A)

F ターム(参考) 5J104 AA07 KA01 NA05 NA33 NA38
NA41 PA07
5K030 GA10 GA15 GA17 HA08 HC01
HD03 JA10 JT03 KA01 KA06
LA08 LB02 LD19
5K033 AA09 CB01 CB08 CB14 CC01
DA01 DA06 DB20 EA03

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

**IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image
problems checked, please do not report these problems to
the IFW Image Problem Mailbox.**